

[UNIX] Bacula Insecure Temporary File Creation and Information Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0102.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/27/05

To: list@securiteam.com

Date: 27 Sep 2005 16:09:32 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Bacula Insecure Temporary File Creation and Information Disclosure

SUMMARY

" <<http://www.bacula.org/>> Bacula is a set of computer programs that permit you (or the system administrator) to manage backup, recovery, and verification of computer data across a network of computers of different kinds."

Bacula fails to generate a random temporary name which in turn allows attackers to perform a symbolic link attacks and retrieve sensitive information.

DETAILS

Vulnerable Systems:

* bacula version 1.36.3 and prior

Immune Systems:

* bacula version 1.37.39

The vulnerabilities caused due to insecure temporary files creations that allow attackers to cause symbolic link attacks to create arbitrary files

Securiteam: [UNIX] Bacula Insecure Temporary File Creation and Information Disclosure

with the privileges of the user running the affected script, sensitive informations disclosure, possible arbitrary commands execution.

Vulnerable code:

autoconf/configure.in:

```
11 tmp=/tmp/p.tmp.$$
12 cp autoconf/randpass.bc $tmp
13 ps | sum | tr -d '[:alpha:]' | sed 's/^k=' >>$tmp
14 date | tr -d '[:alpha:]' | sed 's/^k=k*' >>$tmp
15 ls -l /tmp | sum | tr -d '[:alpha:]' | sed 's/^k=k*' >>$tmp
16 echo "j=s(k); for (i = 0; i < $PWL; i++) r()" >>$tmp
17 echo "quit" >>$tmp
18 bc $tmp | awk -f autoconf/randpass.awk
19 rm $tmp
```

They are 2 vulnerabilities, symlink attack (race condition) and password revelation to untrusted users (race condition). This vulnerability is exploitable on system that doesn't have OpenSSL command.

Vulnerable code:

rescue/linux/getdiskinfo:

```
192 cat >mount_drives <<END_OF_DATA
193 #!/bin/sh
194 #
195 # Mount disk drives --- created by getdiskinfo
196 #
197 END_OF_DATA
198 sed -n 's/^(.*)\ on\ \(.*\) type.*$/mkdir -p \mnt/disk2/p'
$di/mount.ext2.bsi >>mount_drives
199 sed -n 's/^(.*)\ on\ \(.*\) type.*$/mkdir -p \mnt/disk2/p'
$di/mount.ext3.bsi >>mount_drives
200 echo "#" >>mount_drives
201 sed -n 's/^(.*)\ on\ \(.*\) type.*$/mount \1 \mnt/disk2/p'
$di/mount.ext2.bsi >/tmp/1$$
202 sed -n 's/^(.*)\ on\ \(.*\) type.*$/mount \1 \mnt/disk2/p'
$di/mount.ext3.bsi >>/tmp/1$$
203 # sort so that root is mounted first
204 sort -k 3 </tmp/1$$ >>mount_drives
205 rm -f /tmp/1$$
206
207 chmod 755 mount_drives
208
209 # copy sfdisk so we will have it
210 cp -f /sbin/sfdisk .
211 echo "Done building scripts."
212 echo " "
213 echo "You might want to do a:"
214 echo " "
215 echo "chown -R uuuu:gggg *"
216 echo " "
217 echo "where uuuu is your userid and gggg is your group"
```

Securiteam: [UNIX] Bacula Insecure Temporary File Creation and Information Disclosure

218 echo "so that you can access all the files as non-root"
219 echo " "

ADDITIONAL INFORMATION

The information has been provided by <mailto:eromang@zataz.com> Eric Romang.

The original article can be found at:

<<http://www.zataz.net/adviso/bacula-09192005.txt>>

<http://www.zataz.net/adviso/bacula-09192005.txt>

Vendor bug report:

<http://bugs.bacula.org/bug_view_advanced_page.php?bug_id=0000422>

http://bugs.bacula.org/bug_view_advanced_page.php?bug_id=0000422

Gentoo bug report: <http://bugs.gentoo.org/show_bug.cgi?id=104986>

http://bugs.gentoo.org/show_bug.cgi?id=104986

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.